REMARKS

Oath/Declaration

In the Office Action, the Examiner states that the Oath and Declaration filed with this application is defective because it does not contain the signatures of the inventors. Enclosed is a copy of the fully executed Declaration for Patent Application and Power of Attorney, filed with the Response to Notice to File Missing Parts on July 2, 2002. Also enclosed is a copy of the Response, stating the inclusion of the Declaration. Also enclosed is a copy of the return receipt postcard and Express Mail ticket indicating receipt of the Declaration by the United States Patent and Trademark Office. It should also be noted that the Customer Number and correspondence information listed within the Declaration for Patent Application and Power of Attorney is no longer current. The Customer Number and correspondence information should remain associated with Customer Number 36257.

Claim Rejections – 35 USC §112

Claim 2 is objected to because it lacked antecedent basis for the limitation "the audio video device" in the claim. Claim 2 has been canceled without disclaimer and this objection is now therefore moot.

Claims 6, 9 and 32 were rejected under 35 U.S.C. § 112, second paragraph as indefinite and not explicitly defined because of the usage of the word "about" in the claims. It is kindly asserted that usage of the term "about" in these claims does not render the claims indefinite.

The term "about two" envisions some amount of deviation from two. Words of approximation, such as "generally" and "substantially," are descriptive terms "commonly used in patent claims 'to avoid a strict numerical boundary to the specified parameter.'"; see, e.g., Andrew Corp v. Gabriel Elecs. Inc., 847 F.2d 819, 821-22 (Fed. Cir. 1988) (noting that terms such as "approach each other," "close to," "substantially equal," and "closely approximate" are ubiquitously used in patent claims and that such usages, when serving reasonably to describe the claimed subject matter to those of skill in the field of the invention and to distinguish the claimed subject matter from the prior art, have been accepted in patent examination and upheld by the courts).

Anchor Wall Sys. v. Rockwood Retaining Walls, Inc., 340 F.3d 1298, 1310-1311 (Fed. Cir. 2003)(internal citations omitted).

Claim 31 was rejected under 35 U.S.C. §112, second paragraph due to an apparently missing element. Claim 31 has been amended and the claim as amended should no longer suffer from this problem.

Claim Rejections – 35 USC §101

Claims 1-7 and 31-34 were rejected under 35 U.S.C §101 on the basis that the claimed invention is directed to non-statutory subject matter.

These claims have been amended per the Examiner's suggestion, although it is believed that the claimed invention was in fact eligible subject matter. Therefore it is submitted that these claims are now in condition for allowance.

Double Patenting

Claims 23 and 31-34 were provisionally rejected under the doctrine of double patenting. It is submitted that these claims are patentably distinct from the claims in the cited co-pending application, contrary to the Examiner's assertion. The Examiner recognizes that there are differences in the claims, but appears to assert that these differences are so insignificant as to not make any difference in terms of patentability. Firstly the differences sighted by the Examiner are significant. Secondly, there are additional differences in the claims that are apparently not recognized or appreciated by the Examiner. This can be seen in the Examiner's charts on pages 4 and 5 of the current Office Action. For example, among other numerous differences, claim 13 has "means for" terminology where as claim 23 does not. Therefore, by virtue of statute, for this reason alone claim 13 would likely be afforded a different scope than claim 23 under 35 USC § 112. According to the Federal Circuit, double patenting is an affirmative defense, and a must be proven by clear and convincing evidence, "a heavy and unshifting burden." See Symbol Technologies, Inc. v. Opticon, Inc. 935 F.2d 1569 (Fed. Cir. 1991). It is submitted that the cited claims have differences from each other that are not insubstantial, and that Examiner's charts, to the contrary of providing clear and convincing evidence of double patenting, illustrate the numerous differences between the compared claims. Therefore, it is kindly asserted that the claims are not, as submitted or as amended, invalid due to the judicially created doctrine of double patenting.

Claim Rejections – 35 USC §102 and §103

Claims 1-3, 8-22 and 24-29 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,832,293 to Tagawa et al. ("Tagawa"). Claims 4-7, 23, 30-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Tagawa in view of U.S. Patent No. 5,604,801 to Dolan et al. ("Dolan").

Claims 1-3 have been canceled without prejudice or disclaimer. Claim 4 was previously dependent upon claims 1 and 3 and is now in independent form, incorporating some of the limitations of the base claims. Claim 4 was previously rejected under § 103 over Tagawa in view of Dolan.

> 4. A computer readable storage medium having an executable program, the program to be utilized in an audio and/or video device for playback of encrypted audio and/or video files, the program configured to:
>
> decrypt encrypted audio and/or video content of the file from a memory card based on a command received from a user interface of the device, wherein decrypting the audio or video content comprises:
>
> copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device;
>
> copying encrypted audio or video content from the memory card into a memory buffer of the device;
>
> decrypting one or more of the copied encrypted keys;
>
> decrypting the copied encrypted audio or video content with the one or more decrypted keys; and
>
> immediately deleting the one or more decrypted keys after decrypting the audio and/or video content before decrypting additional content of the file.

Neither Tagawa nor Dolan, alone or in combination, teaches all of the limitations of amended claim 4. As the Examiner has stated, Tagawa does not teach "immediately deleting the one or more decrypted keys after decrypting the audio or video content," and Dolan is cited as teaching this limitation. However, Dolan does not teach this limitation, and the combination of Dolan and Tagawa does not therefore teach all of the elements of amended claim 4.

In Dolan, the "invention is directed to the problem of providing a secure method of enabling messages to be processed using public key processing on behalf of the authorised holder of a portable security device, such as a smart card, in such a manner that it can be shown that only the authorised holder of the security device could have authorised the processing of a particular message, without requiring the public key algorithm to be performed by the security device, without having to store the private key in the security device, and without requiring the key generation process to be performed by the security device." Col. 2, lines 54-64.

Dolan in no way teaches an audio and/or video device for playback of encrypted audio and/or video files, or anything to be used in such a device. Dolan teaches a data communications system in which messages are processed using public key cryptography with a private key unique to one or more users 150 under the control of a portable security device 120, such as a smart card, held by each user. Abstract. In Dolan, a workstation 110 incorporating a smart card reader for operation in conjunction with smart card 120 is connected to network 100 as is a server computer 130 and another computer 140 that is the intended recipient of the message. See Col. 5, lines 23-35. Dolan teaches that this system could be used to certify a message such as a debit instruction for the users account, and that generation of a digital signature is performed by server 130. See Col. 5 lines 30-38.

A public key data communications system is very different in purpose and form than the claimed program to be utilized in an audio and/or video device. Much of the security in such a public key system like that taught in Dolan comes from the server. The Examiner cites lines 11-14 of Column 3 of Dolan as teaching the claimed limitation of "immediately deleting the one or more decrypted keys after decrypting the audio and/or video content." In a preceding limitation of the claim, the audio and/or video content is delineated as "of the file from a memory card." In addition to not teaching any audio and/or video content, Dolan also does not teach that any such content is on a memory card. The portable security device of Dolan, which can be a smart card, is never taught to have such content, nor is any decryption of such content on a memory card taught by Dolan. Also, the private key of the public/private key pair that the Examiner appears to equate with the claimed "one or more decrypted keys" in the disputed limitation, is taught to be on a server in Dolan, not a memory card or even the security device of Dolan (which is not taught to store audio and/or video content in any case). Specifically, the cited portion of Dolan teaches a "server comprising secure processing means to receive a message to be processed from the user, retrieve the encrypted private key for the user, decrypt the private key using the key encrypting key and decrypted private key after use..." Figure 3 of Dolan shows the encrypted keys in storage 350 of server 130. This server is in or includes a "secure cryptographic environment 360" that is controlled. Because the server is in or part of a controlled environment, access to the server is limited, unlike the memory card and portable device which are in the hands of a user or potential hacker. Rescinding the ability of user 150 is achieved by deleting the encrypted value of SKa from storage 350 of server 150. See Col. 7, lines 12-24 and Col. 8, lines 31-38. This is very different from claim 4, which has nothing to do with a public key structure that relies on servers with keys in controlled environments to certify messages such as the type used in transactions and other debits. As taught in Dolan itself, "...in such a manner it can be shown that only the authorised holder of the security device could have authorised the processing of a particular message, without requiring the public key algorithm to be performed by the security device, without having to store the private key in the security device, and without requiring the key generation process to be performed by the security device." Col. 2, lines 54-64.

Furthermore, even if the combination of Tagawa and Dolan did teach all the limitations of claim 4, one of skill in the art would not be motivated to make such a combination.

First, as a threshold matter, Dolan is not analogous art and one of skill in the art would therefore not look to Dolan in solving the particular problem at hand. As seen above, Dolan deals with a completely different problem than the claimed invention(s) and described embodiments. The Public Key Data Communications System of Dolan is not relevant to the problem and claimed solution in the present invention, as discussed above (please refer to each claim individually, each of which covers different aspects of the solution and speaks for itself).

Second, there are no specific teachings in either Dolan or Tagawa that would lead one of skill in the art to combine the teachings of the references to arrive at the invention recited in claim 4. Claim 4 has nothing to do with a public key structure that relies on servers with keys in controlled environments to certify messages such as the type used in transactions and other debits.

It seems therefore that such a combination can only be made with the benefit of hindsight, which is impermissible.

Furthermore, in addition to not being particularly relevant to the problem at hand, Dolan actually teaches away from the claimed invention and one of skill in the art would not be motivated to combine its teachings with those of Tagawa. As mentioned above, Dolan teaches "processing of a particular message, without requiring the public key algorithm to be performed by the security device, without having to store the private key in the security device, and without requiring the key generation process to be performed by the security device." Col. 2, lines 54-64.

Therefore, it is submitted that Tagawa, alone or in combination with Dolan does not and cannot anticipate claim 4 under § 102 or render claim 4 obvious under § 103 of 35 USC.

Claims 8-15 have been canceled without prejudice or disclaimer.

Independent claim 16 has been amended and now recites:

> 16. A method of playing encrypted audio or video content stored in a secure media with a device, the method comprising:
> a pre-play process comprising:
> copying one or more groups of information regarding the tracks to be played back into a memory of the device; and
> a play process comprising:
> receiving one more commands from a user interface to initiate playback;
> accessing the one or more groups of information from the memory of device;
> copying approximately less than one to five seconds of encrypted content from the secure media into a memory of the device according to a sequence based upon information of the one or more groups of information copied into the ram memory;
> decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content.

Claims 16 and 17 were rejected under §102 in view of Tagawa. It is submitted that claim 16, as amended to include some portion of claim 17, is not anticipated by Tagawa. Tagawa does not teach "copying approximately less than one to five seconds of encrypted content from the secure media into a memory of the device according to a sequence based upon information of the one or more groups of information copied into the ram memory; and decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content."

While Tagawa does teach that an AOB element has a playback period of around two seconds and that an AOB block has a maximum playback period of 8.4 minutes (Col. 15, lines 32-34), it does not teach, either explicitly or inherently, "copying approximately less than one to five seconds of encrypted content from the secure media into a memory of the device according to a sequence based upon information of the one or more groups of information copied into the ram memory; and decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content." The Examiner has cited Column 15 lines 59-65 of Tagawa for this proposition, but is kindly asserted that neither the cited portion nor any other portion of Tagawa teaches these claim limitations. Tagawa is silent on how much content is copied and decrypted at a time, and therefore how long any encryption key may be in a vulnerable decrypted state.

Therefore, independent claim 16 and claims 18-22 that depend therefrom, are not anticipated by Tagawa and are in condition for allowance.

Claim 23 was rejected as obvious in view of the combination of Tagawa and Dolan. Claim 23 recites:

> 23. A system enabling a portable device to access encrypted music on a memory storage device comprising:
> one or more application programming interfaces configured to:
> receive a plurality of commands from a user interface of the portable device; and
> send commands to an isolated security engine, the isolated security engine configured to:
> receive commands from the application programming interface;
> copy encrypted keys and encrypted content from the memory storage device to a memory of the portable device;
> decrypt the keys;
> decrypt the content using the decrypted keys; and thereafter
> delete the decrypted keys.

The combination of Tagawa and Dolan does not teach all of the limitations of claim 23. The Examiner relies on Dolan for teachings to "delete the decrypted keys." Dolan, however, does not teach the claim limitation when it is taken in context with its antecedent bases, and therefore does not address the insufficient teachings in Tagawa. While Dolan may teach deleting keys, they are not the claimed "decrypted keys."

The antecedent limitations of the claim indicate that the decrypted keys were copied in an encrypted form "from the memory storage device to a memory of the portable device" before being decrypted and deleted. Similar to the discussion above regarding claim 4, Dolan does not teach that the decrypted keys were copied in an encrypted form "from the memory storage device to a memory of the portable device" before being decrypted and deleted. Nor does Dolan teach the claimed "portable device to access encrypted music." Dolan teaches a totally different sort of system where any keys (that can be equated with the claimed keys) that might be deleted reside on a server. As taught in Dolan itself, "...in such a manner it can be shown that only the authorised holder of the security device could have authorised the processing of a particular message, without requiring the public key algorithm to be performed by the security device, without having to store the private key in the security device, and without requiring the key generation process to be performed by the security device." Col. 2, lines 54-64. Thus, Dolan is not teaching about the claimed key manipulation.

Furthermore, even if the combination of Tagawa and Dolan did teach all of the limitations of claim 23, the two references cannot be properly combined because Dolan is not relevant to the problem and is non-analogous art, there is no motivation to combine the references absent impermissible hindsight, and because Dolan in fact teaches away from the combination recited in claim 23 and from Tagawa for reasons similar to those discussed previously.

Additionally, Tagawa, alone or in combination with Dolan, does not teach the limitations of claim 23 of "one or more application programming interfaces configured to: receive a plurality of commands from a user interface of the portable device; and send commands to an isolated security engine, the isolated security engine configured to:..." There is no indication of usage of an application programming interface in Tagawa. As seen in *The Free On-line Dictionary of Computing, © 1993-2005 Denis Howe, available at www.dictionary.com,* an application programming interface, or API is understood by those of skill in the art to mean:

> *<programming> (API, or "application programming interface")*
>
> The interface (calling conventions) by which an application program accesses operating system and other services. An API is defined at source code level and provides a level of abstraction between the application and the kernel (or other privileged utilities) to ensure the portability of the code.
>
> An API can also provide an interface between a high level language and lower level utilities and services which were written without consideration for the calling conventions supported by compiled languages. In this case, the API's main

> task may be the translation of parameter lists from one format
> to another and the interpretation of call-by-value and
> call-by-reference arguments in one or both directions.

Again, neither Tagawa nor Dolan teach the aforementioned limitations that include an API.

Therefore, for all the reasons above, it is submitted that Tagawa, alone or in combination with Dolan does not and cannot anticipate claim 23 under § 102 or render the claim obvious under § 103 of 35 USC.

Claim 24 was rejected as being anticipated by Tagawa. Claim 30 was rejected under § 103 in light of the combination of Tagawa and Dolan. Claim 24 has been amended and now contains limitations previously in dependent claim 30, as seen below.

24. A method for allowing a device having a processor and random access memory to easily access encrypted data from a memory card with a group of commands, the method comprising:

retrieving playlist information from the memory card and storing the information in the random access memory of the device;

retrieving track information from the memory card and storing the track information into the random access memory of the device;

receiving a command selected from the group of commands from the device, the command accessing both of the playlist information, and track information from the random access memory; and

executing the command by retrieving the encrypted data stored within the memory card and decrypting the data based on the accessed information, wherein decrypting the data comprises,

(a) calculating a media unique key; and thereafter
(b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter
(c) decrypting a group of frames; and thereafter
(d) deleting the decrypted title key;
(e) deleting the media unique key; and
(f) repeating (a) through (e) until the entire track is completed.

Tagawa, alone or in combination with Dolan, does not teach all the limitations of claim 24. The Examiner has cited teachings in columns 5, 83, 90, and 94 of Tagawa as teaching element (c) of the claim, however, the highest numbered column of Tagawa is 68, so it is not understood what teachings within Tagawa the Examiner believes teach element (c). Also, in the last paragraph of page 18 of the Office Action the Examiner mentions a reference by the name of Ueda where perhaps the Examiner meant to cite Dolan. This is unclear.

In any case, the combination of Tagawa and Dolan does not teach at least the process delineated in elements (a)-(f). This process is important because it minimizes the exposure of the keys while they are in an unencrypted format, and therefore vulnerable. In particular, Dolan does not teach at least steps (d), (e), and (f), contrary to the Examiner's assertion. Dolan does not teach a title key, let alone deleting a title key, decrypted or not. Dolan does not teach a media unique key, let alone deleting such a key. Dolan also does not teach a track of any kind, let alone repeating steps (a) through (e) until the entire track is completed.

The Examiner's interpretation of "after use" as "until the entire track is completed" on page 18 of the Office Action cannot stand. Firstly, it is an incomplete assertion and ignores the repeating of steps (a) through (e), which is not a superfluous part of step (f) and the overall process and involves performing complex processes in an orderly fashion. Secondly, there is no basis within Dolan that can support such an interpretation. As mentioned above, Dolan does not teach a track of any kind, let alone repeating steps (a) through (e) until the entire track is completed. This interpretation appears to rely on the benefit of hindsight.

Furthermore, even if the combination of Tagawa and Dolan did teach all of the limitations of the claim, Tagawa and Dolan cannot be properly combined. As discussed previously, Dolan is not relevant to the problem and is non-analogous art, the two references cannot be properly combined because there is no motivation to combine the references absent impermissible hindsight, and Dolan in fact teaches away from the combination recited in the claim and from Tagawa. Please refer back to previous arguments explaining why this is the case.

Therefore, it is submitted that Tagawa, alone or in combination with Dolan does not and cannot anticipate claim 24 and the claims that depend therefrom under § 102 or render the claim obvious under § 103 of 35 USC.

Independent claim 31 was rejected under § 103 in view of the combination of Tagawa and Dolan. Claim 31, as amended, can be seen below.

31. A software system that enables a device to access content on a secure medium comprising:

one or more user interface modules for receiving commands from the device;

an applications programming interface for receiving the commands from the user interface module(s) and managing the retrieval and storage of both encrypted and non encrypted content from the secure medium;

a security engine for decrypting the encrypted content and encrypted keys sent from the secure medium to memory of the device, the decrypted keys used to decrypt the encrypted content, and wherein

one or more of the keys are contained in a first encrypted data segment, and encrypted content is contained in a second encrypted data segment, and

the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting another portion of the first encrypted data segment, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content.

Tagawa, alone or in combination with Dolan, does not teach at least the claim limitations of "a security engine for decrypting the encrypted content and encrypted keys sent from the secure medium to memory of the device, the decrypted keys used to decrypt the encrypted content, and wherein one or more of the keys are contained in a first encrypted data segment, and encrypted content is contained in a second encrypted data segment, and the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting another portion of the first encrypted data segment, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content."

While Tagawa does teach that an AOB element has a playback period of around two seconds and that an AOB block has a maximum playback period of 8.4 minutes (Col. 15, lines 32-34), neither Tagawa nor Dolan teaches, either explicitly or inherently, the limitations that "one or more of the keys are contained in a first encrypted data segment, and encrypted content is contained in a second encrypted data segment, and the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting another portion of the first encrypted data segment, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content."

Furthermore, even if the combination of Tagawa and Dolan did teach all of the limitations of the claim, Tagawa and Dolan cannot be properly combined. As discussed previously, Dolan is not relevant to the problem and is non-analogous art, the two references cannot be properly combined because there is no motivation to combine the references absent impermissible hindsight, and Dolan in fact teaches away from the combination recited in the claim and from Tagawa.

Therefore, it is submitted that Tagawa, alone or in combination with Dolan does not and cannot anticipate claim 31 and the claims that depend therefrom under § 102 or render the claim obvious under § 103 of 35 USC.

Information Disclosure Statement

An information disclosure statement is filed along with this Response to submit newly cited references from a related case.

Conclusion

Accordingly, it is believed that this application is now in condition for allowance and an early indication of its allowance is solicited. However, if the Examiner has any further matters that need to be resolved, a telephone call to the undersigned attorney at 415-318-1163 would be appreciated.

Respectfully submitted,

Gerald P. Parsons Reg. No. 24,486	October 6, 2005 Date

PARSONS HSUE & DE RUNTZ LLP
595 Market Street, Suite 1900
San Francisco, CA 94105
(415) 318-1160 (main)
(415) 318-1163 (direct)
(415) 693-0194 (fax)